United Nations A/CN.9/WG.IV/WP.149

General Assembly

Distr.: Limited
31 January 2018

Original: English

United Nations Commission on International Trade Law
Working Group IV (Electronic Commerce)
Fifty-sixth session
New York, 16–20 April 2018

Legal Issues Related to Identity Management and Trust Services

Note by the Secretariat

Contents

		Page
I.	Introduction	2
II.	Relevant Issues for Future Work on Legal Aspects of Identity Management and Trust Services	3

V.18-00419 (E)

Please recycle

I. Introduction

1. At its forty-eighth session, in 2015, the Commission requested the Secretariat to conduct preparatory work on legal aspects of identity management and trust services, including through the organization of colloquia and expert group meetings, for future discussion at the Working Group level following the completion of work on electronic transferable records on the basis of a proposal submitted to the Commission for its consideration (A/CN.9/854).[1]

2. At that session, the Commission also asked the Secretariat to share the result of such preparatory work with Working Group IV, with a view to seeking recommendations on the exact scope, possible methodology and priorities for the consideration of the Commission at its forty-ninth session.[2]

3. At its forty-ninth session, in 2016, the Commission had before it a note by the Secretariat on legal issues related to identity management and trust services (A/CN.9/891) summarizing the discussions during the UNCITRAL Colloquium on Legal Issues Related to Identity Management and Trust Services held in Vienna on 21 and 22 April 2016 and complemented by other material.

4. At that session, the Commission agreed that the topics of identity management and trust services, as well as of cloud computing, should be retained on the work agenda of the Working Group and that it would be premature to prioritize between the two topics. The Commission confirmed its decision that the Working Group could take up work on those topics upon completion of the work on the Model Law on Electronic Transferable Records. In that context, the Secretariat, within its existing resources, and the Working Group were asked to continue to update and conduct preparatory work on the two topics including their feasibility in parallel and in a flexible manner and report back to the Commission so that it could make an informed decision at a future session, including the priority to be given to each topic. [3]

5. At its fifty-fourth session (Vienna, 31 October–4 November 2016), the Working Group held a preliminary exchange of view on its possible future work on legal aspects of identity management and trust services.

6. At that session the Working Group agreed that such future work should be limited to the use of identity management systems for commercial purposes and that it should not take into account the private or public nature of the identity management services provider. The Working Group also agreed that, while work on identity management could be taken up before work on trust services, the identification and definition of terms relevant for identity management and trust services should take place simultaneously given the close relationship between the two. It was further agreed that focus should be placed on multi-party identity systems and on natural and legal persons, without excluding consideration of two-party identity systems and of physical and digital objects when appropriate. In addition, it was agreed that the Working Group should continue its work by further clarifying the goals of the project, specifying its scope, identifying applicable general principles and drafting necessary definitions (A/CN.9/897, paras. 118–120 and 122).

7. At its fifty-fifth session (New York, 24–28 April 2017), the Working Group discussed various aspects of its possible future work on legal aspects of identity management and trust services. In particular, at that session the Working Group discussed the objectives of the project, the general principles inspiring the project and the possible subjects to be addressed by future work.

8. At its fiftieth session, in 2017, after discussion the Commission reaffirmed the mandate given to the Working Group at its forty-ninth session, in 2016

[1] *Official Records of the General Assembly, Seventieth Session, Supplement No. 17* (A/70/17), paras. 354–355 and 358.

[2] Ibid, para. 358.

[3] Ibid, *Seventy-first Session, Supplement No. 17* (A/71/17), para. 229.

(see para. 4 above). It agreed to revisit that mandate at its fifty-first session, in particular if the need arose to prioritize between the topics or to give a more specific mandate to the Working Group as regards its work in the area of identity management and trust services. The Secretariat was requested to consider convening expert group meetings as it deemed necessary to expedite the work in both areas and ensure the productive use of conference resources by the Working Group. States and international organizations were invited to share with the Working Group and the Secretariat their expertise in the areas of work assigned to the Working Group.

9. The Secretariat convened an expert group meeting on legal aspects of identity management and trust services in Vienna on 23 and 24 November 2017. This note, based on comments made on that occasion as well as other relevant material, is submitted to the Working Group to facilitate further discussion on the scope and goals of possible future work in that field.

II. Relevant Issues for Future Work on Legal Aspects of Identity Management and Trust Services

10. The fundamental importance of identity management ("IdM") and trust services for all types of electronic transaction has been repeatedly noted. In particular, the desirability of preparing adequate legal tools to facilitate mutual legal recognition and, more generally, clarify the legal status of IdM and trust services has been suggested. Hence, support has been expressed for conducting work in support of establishing an enabling environment for IdM and trust services.

11. The emergence of different approaches, reflected in national and regional legislation, has also been noted. Taking into account existing legislation, it has been suggested that guidance should be given to prevent fragmentation that could hinder cross-border transactions. In that respect, the interrelation between mutual legal recognition and technical interoperability has been stressed.

12. However, the view has also been expressed that any project in the field should have a clearly recognizable impact on legal issues. In that respect, it was indicated that the overarching goal should be to identify legal obstacles to the use of IdM and trust services and prepare tools to overcome them.

13. With respect to work on IdM, two possible approaches have been identified. The first approach suggests that guidance should be given on fundamental issues related to the legal effects of IdM, including, but not limited to, cross-border ones (A/CN.9/902, para. 34). The second approach recommends focusing on cross-border issues, in the context of a commonly-understood framework of reference (A/CN.9/902, para. 32).

14. The two approaches share common elements, including applicable general principles. Those general principles have been identified as: technological neutrality, including with respect to economic and system models; functional equivalence, to the extent applicable; non-discrimination against the use of electronic means; and party autonomy (A/CN.9/902, paras. 52, 54 and 63).

15. Moreover, both approaches focus on addressing matters specific to IdM and trust services. Other laws, e.g. laws generally applicable to commercial transactions or to electronic transactions, would not be affected. Moreover, parties to a commercial transaction may decide to agree on specific IdM rules. Those contractual rules may be particularly relevant in the context of federated IdM systems. Both approaches aim at supporting enforceability of contractual rules.

16. With respect to the first approach, suggesting that guidance should be given on fundamental issues related to the legal effects of IdM, several possibly relevant topics have been identified. Those topics include: legal recognition, mutual recognition, attribution of identity information, attribution of actions, liability and risk allocation, and transparency. Those topics may be relevant also for a discussion of legal issues

related to trust services. The Working Group may wish to recall its preliminary discussion of those topics (A/CN.9/902, paras. 66–85).

17. Should that approach be followed, it was suggested that work could commence by identifying cases where IdM was used. In that respect, it should be noted that identification may be required for different purposes. Reference is often made to regulatory compliance. One example of such requirement is the application of "Know Your Customer" (KYC) rules in the finance, telecom and other business sectors. Another example may be found in the field of electronic procurement, where the correct identification of potential vendors is necessary, for instance, to prevent fraud and collusion and to enforce debarment.

18. Moreover, identification may be required for the validity of a commercial document. For instance, the law applicable to a bill of lading may require the identification of certain parties (see e.g. art. 15 of the Hamburg Rules[4] and art. 36 of the Rotterdam Rules[5]).

19. Lastly, parties to a transaction may have an interest in identifying each other online accurately and may agree on the use of certain procedures and methods to achieve that goal. The source of that duty to identify is therefore contractual.

20. Another potentially relevant issue under this approach is the desirability and feasibility of formulating a functional equivalence rule for the notion of "identification" on the basis of paper-based documents or similar credentials.

21. The second approach envisages facilitating a common understanding on how existing IdM systems, including their legal framework, may interact. Under that approach, existing identification schemes would not be affected; however, a tool would be created to achieve mutual legal recognition among those schemes.

22. Discussions on that second approach highlighted how a model based on a centrally-managed licensing system may pose challenges at the global level. In particular, governance of that licensing system could be complex and costly. Moreover, a centrally-managed system may not be reacting to developments as quickly as technological evolution may require, thus possibly hindering innovation. Hence, it was suggested that alternative solutions should be explored.

23. One suggestion made reference to the possibility of mapping IdM systems according to a common template. Referring to generic description of levels of assurance could ensure that exercise would be outcome-based, which, in turn, would preserve the application of the principle of technological neutrality. Guidance could be provided also on the mapping exercise, which could be carried out by any concerned party, including private and commercial entities.

24. Elements possibly relevant for the mapping exercise may be identified in the Commission Implementing Regulation (EU) 2015/1502, operating in the framework of the eIDAS Regulation.[6] Those elements are: enrolment, electronic identification means management, authentication, and management and organization. Each element includes several sub-elements.

25. The legal effects of the mapping exercise would be defined by the scheme in which the IdM tool is supposed to operate. In that respect, the Working Group may wish to consider the desirability and feasibility of possible discussions on definitions of levels of assurance and legal consequences thereof. Similarly, the Working Group may wish to consider if, and to what extent, guidance could be provided on specifications and procedures to be followed in the mapping exercise.

---

[4] United Nations, *Treaty Series*, vol. 1695, No. 29215, p. 3.

[5] General Assembly resolution 63/122, annex.

[6] Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

26. A practical example may illustrate how the mapping exercise might work. As noted above, KYC requirements are common in various business sectors. Those requirements may not be satisfied by using identity credentials issued in a different jurisdiction without a formal mechanism for mutual recognition of IdM schemes. In the absence of such mechanism, the foreign credentials could be mapped against generic descriptions of levels of assurance. It would thus be possible to verify whether the suggested foreign identity credentials could satisfy the requirements for the level of assurance needed for KYC purposes.

27. The level of assurance for enrolment where KYC requirements are applied may be higher than the level of assurance required for carrying out remote banking transactions, and significantly higher than those required for accessing a mobile telephone. Under the suggested approach, different foreign credentials could be used in a flexible manner to satisfy the various identification needs.

28. Certain issues may be relevant in defining the scope of possible future work of the Working Group regardless of the recommended approach. One such issue is whether the scope of work should be limited to commercial transactions, or extend to transactions with other entities, to the extent that those are relevant for business (e.g., identification in the context of paperless trade facilitation), or cover all forms of identification regardless of the nature of the transaction.

29. In that respect, it may be useful to take into consideration the distinction between primary determination of identity (also called foundational identity) and secondary determination of identity (also called transactional or functional identity). The primary determination of identity may raise complex issues of status attribution. However, commercial transactions may rely, in full or in part, on a secondary determination of identity. The actual legal consequences of identity verification would be determined by factual and other relevant circumstances of the specific transaction.

30. With regard to possible future work on legal issues relating to trust services, support was expressed for closely coordinating that work with work on IdM. The suggestion was also made that such work should consider an open-ended list of trust services based on a common definition of "trust service".

31. The Working Group may recall the Commission's request to the Working Group to continue updating and conducting preparatory work on legal aspects of IdM and trust services, including with respect to feasibility, and to report back to the Commission to enable it to make an informed decision at its next session (see paras. 4 and 8 above).

32. In light of that request, the Working Group may wish to formulate a recommendation to the Commission on future work in the field of IdM and trust services. That recommendation might indicate the details of the work to be undertaken, the form it might take and how it might best be progressed, including the possibility of adopting a flexible approach to working methods. In formulating that recommendation, the Working Group may wish to take into account:

(a) The potential legal effect of such work on removing obstacles to the broader use of IdM and trust services and preventing the creation of new obstacles;

(b) Types of electronic transactions to be covered, in particular involvement of non-commercial entities;

(c) Possible legal treatment of legal recognition, attribution of identity information, attribution of actions, liability and risk allocation, and transparency in the context of IdM and trust services; and

(d) Cross-border aspects, namely mutual recognition and elements relevant for a mapping exercise such as enrolment, electronic identification means management, authentication, and management and organization.

33. Additional considerations on legal aspects of IdM and trust services may be found in documents A/CN.9/WG.IV/WP.141, A/CN.9/WG.IV/WP.144, A/CN.9/WG.IV/WP.145 and A/CN.9/WG.IV/WP.146 as well as in documents A/CN.9/891 and A/CN.9/902.

United Nations A/CN.9/WG.IV/WP.150

General Assembly

Distr.: Limited
6 February 2018

Original: English

United Nations Commission on International Trade Law
Working Group IV (Electronic Commerce)
Fifty-sixth session
New York, 16–20 April 2018

Legal issues related to identity management and trust services

Terms and concepts relevant to identity management and trust services

Note by the Secretariat

Contents

		Page
I.	Introduction	2
II.	Terms and concepts relevant to identity management and trust services	3
	A. Definitions relevant to identity management	3
	B. Definitions relevant to trust services	9

V.18-00557 (E)

Please recycle

I. Introduction

1. At its forty-eighth session, in 2015, the Commission instructed the Secretariat to conduct preparatory work on identity management and trust services, cloud computing and mobile commerce, including through the organization of colloquia and expert group meetings, for future discussion at the Working Group level. The Commission also asked the Secretariat to share the result of that preparatory work with Working Group IV, with a view to seeking recommendations on the exact scope, possible methodology and priorities for the consideration of the Commission at its forty-ninth session.[1]

2. At its forty-ninth session, in 2016, the Commission had before it a note by the Secretariat on legal issues related to identity management and trust services (A/CN.9/891) summarizing the discussions during the UNCITRAL Colloquium on Legal Issues Related to Identity Management and Trust Services held in Vienna on 21 and 22 April 2016 and complemented by other material. The Commission was also informed that work on contractual aspects of cloud computing had started at the expert level on the basis of a proposal (A/CN.9/856) submitted at the forty-eighth session of the Commission, in 2015.

3. At that session, the Commission agreed that the topics of identity management and trust services, as well as of cloud computing, should be retained on the work agenda of the Working Group and that it would be premature to prioritize between the two topics. The Commission confirmed its decision that the Working Group could take up work on those topics upon completion of the work on the Model Law on Electronic Transferable Records. In that context, the Secretariat, within its existing resources, and the Working Group were asked to continue to update and conduct preparatory work on the two topics including their feasibility in parallel and in a flexible manner and report back to the Commission so that it could make an informed decision at a future session, including the priority to be given to each topic.[2]

4. At its fiftieth session, in 2017, after discussion the Commission reaffirmed the mandate given to the Working Group at its forty-ninth session, in 2016 (see para. 3 above). It agreed to revisit that mandate at its fifty-first session, in particular if the need arose to prioritize between the topics or to give a more specific mandate to the Working Group as regards its work in the area of identity management and trust services.[3]

5. At its fifty-fifth session (New York, 24–28 April 2017), the Working Group had before it a note listing terms and concepts relevant to identity management and trust services (A/CN.9/WG.IV/WP.143). At that session, the Working Group asked the Secretariat to revise that note by including definitions and concepts listed in paragraph 20 of document A/CN.9/WG.IV/WP.144.[4]

6. This note contains the definition of a number of terms relevant for identity management and trust services. The terms are presented with a view to enabling discussions based on a common understanding of fundamental notions; they are not presented in order to suggest a discussion on legally binding definitions of those notions. Similarly, the terms are not intended to provide an indication on the scope of the future work of UNCITRAL in the field of identity management and trust services.

7. The source of the defined terms, where available, is explicitly indicated. Due to different sources, the same term may include more than one definition. If no source is indicated, the definition was suggested during expert consultations. Preference was given to terms defined internationally. Additional sources of defined terms are available, especially at the national level.

---

[1] *Official Records of the General Assembly, Seventieth Session, Supplement No. 17* (A/70/17), para. 358.

[2] Ibid., *Seventy-first Session, Supplement No. 17* (A/71/17), para. 229.

[3] Ibid., *Seventy-second Session, Supplement No. 17* (A/72/17), para. 127.

[4] A/CN.9/902, para. 92.

8. The defined terms are listed in different sections for ease of presentation only and without prejudice to the determinations of the Working Group on their relevance for discussions on the legal aspects of identity management or of trust services.

9. The defined terms have different origins and therefore should not be read as a coherent set of interconnected terms. Rather, each term should be read separately as a stand-alone definition and as such is presented as a possible reference for the discussions of the Working Group. When available, the source of the defined term is indicated so that additional information could be gathered from the original source document.

10. Synonyms are indicated for convenience only in light of usage. Not all synonyms are terms defined in this note.

11. The terms are listed in alphabetical order in the English language version of this note. The same order is maintained in other language versions to ensure correspondence of paragraphs and therefore facilitate reference during the Working Group discussions.

II. Terms and concepts relevant to identity management and trust services

A. Definitions relevant to identity management

12. "Assurance level" means a level of confidence in the binding between an entity and the presented identity information. Source: Rec. ITU-T X.1252. Synonyms: identity assurance, level of assurance.

13. "Attribute" means an item of information or data associated with a subject. Examples of attributes include information such as name, address, age, gender, title, salary, net worth, driver's license number, social security number, email address, mobile number, and data such as the subject's network presence, the device used by the subject, the subject's usual home location as known by a network, etc. (for a human being); corporate name, principal office address, registration name, jurisdiction of registration, etc. (for a legal entity); make and model, serial number, location, capacity, device type, etc. (for a device). Synonym: identity attribute.

14. "Attribute provider" means a business or government entity that acts as a source of one or more attributes of a subject's identity. An attribute provider is often the entity responsible for assigning, collecting, or maintaining such attributes. Examples of attribute providers include a government agency that maintains a birth registry or title registry, a national credit bureau, a business that maintains a commercial marketing database or a corporate registry, and entities such as mobile operators, banks, utilities and healthcare providers that hold verified user data and that either verify or provide these attributes to third parties (possibly, subject to user consent).

15. "Authentication" means (a) a process used to achieve sufficient confidence in the binding between the entity and the presented identity. Source: Rec. ITU-T X.1252; (b) the process of associating the claimed identity of a subject with the actual subject by confirming the subject's association with a credential either directly (active authentication) or through the environment in which the subject is interacting ("passive authentication" or "adaptive authentication"). For example, entering a secret password that is associated with a username is assumed to authenticate that the individual entering the secret password is the person to whom the username was issued. Likewise, comparing a person presenting a passport to the picture appearing on the passport is used to authenticate (i.e., confirm) that that person is the person described in the passport; (c) an electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed. Source: eIDAS, article 3(5). (See also A/CN.9/WG.IV/WP.144, para. 20.)

16. "Authentication assurance" means the degree of confidence reached in the authentication process that the communication partner is the entity that it claims to be or is expected to be. Note: the confidence is based on the degree of confidence in the binding between the communicating entity and the identity that is presented. Source: Rec. ITU-T X.1252. Note: in some cases, the notions of "identity assurance" and "authentication assurance" are viewed as separate components of the overall concept of "level of assurance".

17. "Authentication factor" means (a) a piece of information and process used to authenticate or verify the identity of an entity. Source: ISO/IEC 19790. Note: authentication factors are divided into four categories: (i) something an entity has (e.g., device signature, passport, hardware device containing a credential, private key); (ii) something an entity knows (e.g., password, PIN); (iii) something an entity is (e.g., biometric characteristic); or (iv) something an entity typically does (e.g., behaviour pattern). Source: Rec. ITU-T X.1254; (b) a factor confirmed as being bound to a person, which falls into any of the following categories: (i) 'possession-based authentication factor' means an authentication factor where the subject is required to demonstrate possession of it; (ii) 'knowledge-based authentication factor' means an authentication factor where the subject is required to demonstrate knowledge of it; (iii) 'inherent authentication factor' means an authentication factor that is based on a physical attribute of a natural person, and of which the subject is required to demonstrate that they have that physical attribute. Source: Commission Implementing Regulation (EU) 2015/1502, Annex, article 1(2).

18. "Authenticator" means something that is used to verify the relationship between a subject and a credential. An active authenticator is usually something the subject knows (such as a secret password), something the subject has (such as a smartcard), or something the subject is (such as a photo or other biometric information), and is used to tie the subject to an identity credential. For example, a password functions as an authenticator for a username, a picture functions as an authenticator for a passport or driver's license. A passive authenticator is usually something the environment knows, e.g. the mobile network knows that the user is connected to the network, is in the usual location, is using the usual mobile device, has not been barred from using the network, etc.

19. "Authoritative source" means (a) a repository which is recognized as being an accurate and up-to-date source of information. Source: Rec. ITU-T X.1254; (b) any source irrespective of its form that can be relied upon to provide accurate data, information and/or evidence that can be used to prove identity. Source: Commission Implementing Regulation (EU) 2015/1502, Annex, article 1(1). (See also A/CN.9/WG.IV/WP.144, para. 20.)

20. "Authorization" means (a) a process of granting rights and privileges to an authenticated subject based on criteria usually determined by the relying party. For example, once a subject is authenticated, he or she might be granted access to a confidential database. Source: A/CN.9/WG.IV/WP.120, annex; (b) the granting of rights and, based on these rights, the granting of access. Source: Rec. ITU-T Y.2720 and Rec. ITU-T X.800.

21. "Credential" means (a) a set of data presented as evidence of a claimed identity and/or entitlements. Source: Rec. ITU-T X.1252; (b) data in digital or tangible form presented as evidence of a claimed identity of a subject. Examples of paper-based credentials include passports, birth certificates, driver's licenses, and employee identity cards. Examples of digital credentials include usernames, smart cards, mobile identity and digital certificates. Source: A/CN.9/WG.IV/WP.120, annex. Synonyms: electronic identification means, identity credential.

22. "Credential provider" or "Credential service provider" means (a) an entity that issues credentials to subjects; (b) a trusted actor that issues and/or manages credentials. Note: the Credential Service Provider (CSP) may encompass Registration Authorities (RAs) and verifiers that it operates. A CSP may be an independent third party, or it may issue credentials for its own use. Source: Rec. ITU-T X.1254.

23. "Electronic identification" means the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person. Source: eIDAS, article 3(1). (See also A/CN.9/WG.IV/WP.144, para. 20.)

24. "Electronic identification means" means a material and/or immaterial unit containing person identification data and which is used for authentication for an online service. Source: eIDAS, article 3(2). (See also A/CN.9/WG.IV/WP.144, para. 20.)

25. "Electronic identification scheme" means a system for electronic identification under which electronic identification means are issued to natural or legal persons, or natural persons representing legal persons. Source: eIDAS, article 3(4). (See also A/CN.9/WG.IV/WP.144, para. 20.)

26. "Enrolment" means (a) the process of inauguration of an entity into a context. Note 1: enrolment may include verification of the entity's identity and establishment of a contextual identity. Note 2: also, enrolment is a pre-requisite to registration. In many cases, the latter is used to describe both processes. Source: Rec. ITU-T X.1252; (b) the process by which credential providers (or their agents) verify the identity claims of a subject before issuing a credential to such subject.

27. "Entity" means something that has separate and distinct existence and that can be identified in a context. Note: an entity can be a physical person, an animal, a juridical person, an organization, an active or passive thing, a device, a software application, a service, etc., or a group of these entities. In the context of telecommunications, examples of entities include access points, subscribers, users, network elements, networks, software applications, services and devices, interfaces, etc. Source: Rec. ITU-T X.1252. An entity may have multiple identifiers.

28. "Federation" means (a) an association of users, service providers, and identity service providers. Source: Rec. ITU-T X.1252; (b) a group of identity providers, relying parties, subjects and others that agree to operate under compatible policies, standards, and technologies specified in system rules (or a trust framework) in order that subject identity information provided by identity providers can be understood and trusted by relying parties. Synonyms: identity federation, multi-party identity system.

29. "Identification" means the process of collecting, verifying, and validating sufficient identity attributes about a specific subject to define and confirm its identity within a specific context. Synonyms: identity proofing, registration.

30. "Identifier" means (a) one or more attributes used to identify an entity within a context. Source: Rec. ITU-T X.1252; (b) one or more attributes that uniquely characterize an entity in a specific context. Source: Rec. ITU-T X.1254.

31. "Identity" means (a) a set of attributes related to an entity. Source: ISO/IEC 24760; (b) information about a specific subject in the form of one or more attributes that allow the subject to be sufficiently distinguished within a particular context; (c) a set of the attributes about a person that uniquely describes the person within a given context. Synonym: digital identity.

32. "Identity assertion" means an electronic record originating with an identity provider and sent to a relying party that contains the subject's identifier (e.g., name, account number, mobile number, location, etc.), authentication status, and applicable identity attributes. The attributes are typically personal and non-personal information about the subject that is relevant to the transaction required by the relying party.

33. "Identity assurance" means the degree of confidence in the process of identity validation and verification used to establish the identity of the entity to which the credential was issued, and the degree of confidence that the entity that uses the credential is that entity or the entity to which the credential was issued or assigned. Source: Rec. ITU-T X.1252. Synonyms: assurance level; level of assurance. Note: in some cases, the notions of "identity assurance" and "authentication assurance" are viewed as separate components of the overall concept of "level of assurance".

34. "Identity federation" means a group of identity providers, relying parties, subjects and others that agree to operate under compatible policies, standards, and technologies specified in system rules (or a trust framework) in order that subject identity information provided by identity providers can be understood and trusted by relying parties. See also: federation; multi-party identity system.

35. "Identity management" means (a) a set of processes to manage the identification, authentication, and authorization of individuals, legal entities, devices, or other subjects in an online context. Source: A/CN.9/854, paragraph 6; (b) a set of functions and capabilities (e.g., administration, management and maintenance, discovery, communication exchanges, correlation and binding, policy enforcement, authentication and assertions) used for: (i) assurance of identity information (e.g., identifiers, credentials, attributes); (ii) assurance of the identity of an entity; and (iii) enabling business and security applications. Source: Rec. ITU-T Y.2720.

36. "Identity proofing" means (a) the process of collecting, verifying, and validating sufficient identity attribute information about a specific subject (a person, legal entity, device, digital object, or other entity) to define and confirm its identity within a specific context. Identity proofing may be carried out through self-assertion or against existing records; (b) a process which validates and verifies sufficient information to confirm the claimed identity of the entity. Source: Rec. ITU-T X.1252; (c) a process by which a registration authority (RA) captures and verifies sufficient information to identify an entity to a specified or understood level of assurance. Source: Rec. ITU-T X.1254. Synonyms: identification; registration.

37. "Identity provider" means (a) an entity responsible for the identification of persons, legal entities, devices, and/or digital objects, the issuance of corresponding identity credentials, and the maintenance and management of such identity information for subjects. Source: A/CN.9/WG.IV/WP.120, annex; (b) an entity that creates, maintains and manages trusted identity information of other entities (e.g., users/subscribers, organizations and devices) and offers identity-based services based on trust, business and other types of relationship. Source: Rec. ITU-T Y.2720. Synonym: credential service provider; identity service provider.

38. "Identity system" means an online environment for identity management transactions governed by a set of system rules (also referred to as a trust framework) where individuals, organizations, services, and devices can trust each other because authoritative sources establish and authenticate their identities. Source: A/CN.9/WG.IV/WP.120, annex. An identity system involves (a) a set of rules, methods, procedures and routines, technology, standards, policies, and processes, (b) applicable to a group of participating entities, (c) governing the collection, verification, storage, exchange, authentication, and reliance on identity attribute information about an individual person, a legal entity, device, or digital object, (d) for the purpose of facilitating identity transactions. Synonyms: identity management system ("IdM system"); identity federation; electronic identification scheme; information security management system.

39. "Identity transaction" means any transaction involving two or more participants which involves establishing, verifying, issuing, asserting, revoking, communicating, or relying on identity information.

40. "Identity verification" means the process of confirming that a claimed identity is correct by comparing the offered claims of identity with previously proven information. Source: Rec. ITU-T X.1252.

41. "Information security management system" means a set of processes and procedures designed to manage to acceptable levels risks related to information security. Source: Commission Implementing Regulation (EU) 2015/1502, Annex, article 1(1).

42. "Level of assurance" means a designation of the degree of confidence in the identification and authentication processes — i.e., (a) the degree of confidence in the vetting process used to establish the identity of an entity to whom a credential was

issued, and (b) the degree of confidence that the entity using the credential is the entity to whom the credential was issued. The assurance reflects the reliability of methods, processes and technologies used. Some level of assurance schemes define levels of assurance by number, i.e., Levels 1 to 4, where Level 1 is the lowest assurance level, and Level 4 is the highest. Other schemes designate assurance levels as "low," "substantial" and "high". Synonyms: assurance level; identity assurance; trust level.

43. "Multifactor authentication" means authentication with at least two independent authentication factors. Note: authentication factors are divided into four categories: (a) something an entity has (e.g., device signature, passport, hardware device containing a credential, private key); (b) something an entity knows (e.g., password, PIN); (c) something an entity is (e.g., biometric characteristic); or (d) something an entity typically does (e.g., behaviour pattern). Source: ISO/IEC 19790; Rec. ITU-T X.1254.

44. "Multi-party identity system" means an identity system, also referred to as an identity federation, in which a subject can use an identity credential issued by any one of several identity providers to authenticate multiple unrelated relying parties: An identity system that allows the use of identity credentials issued, and identity information asserted, by one or more identity providers with multiple relying parties. Source: A/CN.9/WG.IV/WP.120, annex. Synonym: identity federation.

45. "Participant" means any person or legal entity that participates in an identity system or an identity transaction using such system. Participants include subjects, identity providers, attribute providers, credential providers, relying parties, identity system operators, and others. Like participants in a credit card system, participants in an identity system typically agree contractually to a set of system rules (often referred to as a trust framework) applicable to their role.

46. "Person identification data" means a set of data enabling the identity of a natural or legal person, or a natural person representing a legal person to be established. Source: eIDAS, article 3(3). (See also A/CN.9/WG.IV/WP.144, para. 20.)

47. "Proofing" means the verification and validation of information when enrolling new entities into identity systems. Source: Rec. ITU-T X.1252. Synonyms: identity proofing, identification.

48. "Pseudonym" means an identifier whose binding to an entity is not known or is known to only a limited extent, within the context in which it is used. Note: a pseudonym can be used to avoid or reduce privacy risks associated with the use of identifier bindings which may reveal the identity of the entity. Source: Rec. ITU-T X.1252.

49. "Registration" means a process in which an entity requests and is assigned privileges to use a service or resource. Note: enrolment is a pre-requisite to registration. Enrolment and registration functions may be combined or separate. Source: Rec. ITU-T X.1252.

50. "Registration authority" means an entity that provides enrolment and/or identity proofing services in the context of a federated (i.e., multi-party) identity system, usually for an identity provider.

51. "Relying party" means (a) the person or legal entity that relies on an identity credential or identity assertion to make a decision as to what action to take in a given application context, such as to process a transaction or grant access to information or a system. Source: A/CN.9/WG.IV/WP.120, annex; (b) an entity that relies on an identity representation or claim by a requesting/asserting entity within some request context. Source: Rec. ITU-T X.1252; (c) a natural or legal person that relies upon an electronic identification or a trust service. Source: Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC ("eIDAS"), article 3(6).

52. "Repository" means an interface that accepts deposits of digital entities, enables their retention, and provides secure access to the digital entities via their identifiers. Source: Rec. ITU-T X.1255.

53. "Role" means a type (or category) of participant in an identity system, such as a subject, identity provider, credential provider, relying party, etc. A participant may have multiple roles. For example, with respect to the identification of its employees, an employer may function as both an identity provider and a relying party.

54. "Self-asserted identity" means an identity that an entity declares to be its own. Source: Rec. ITU-T X.1252.

55. "Subject" means the person, legal entity, device, or digital object (i.e., the entity) that is identified in a particular identity credential and that can be authenticated and vouched for by an identity provider. Source: A/CN.9/WG.IV/WP.120, annex. Synonyms: user; data subject.

56. "System rules": see trust framework.

57. "Trust" means the firm belief in the reliability and truth of information or in the ability and disposition of an entity to act appropriately, within a specified context. Source: Rec. ITU-T X.1252.

58. "Trust framework" means (a) the system rules for an identity system consisting of the business, technical, and legal rules that govern the participation in and operation of a specific identity system. They are typically privately developed (e.g., by the identity system operator of a specific identity system), and made binding and enforceable on the participants via contract. Source: A/CN.9/WG.IV/WP.120, annex; (b) a set of requirements and enforcement mechanisms for parties exchanging identity information. Source: Rec. ITU-T X.1254; (c) an IdM system where a set of verifiable commitments made by each of the various parties in a transaction to their counter parties, and these commitments necessarily include: (i) controls to help ensure commitments are met and (ii) remedies for failure to meet such commitments. Source: Rec. ITU-T X.1255. Synonyms: system rules; operating rules; scheme rules.

59. "Trust framework provider" means the entity or organization that creates or adopts the system rules and associated contractual structure for a specific identity system. The trust framework provider may also certify the participants that are in compliance with those system rules. For example, credit and debit card issuers may fulfill a similar role in the credit and debit card world; they set forth the system rules and enforce compliance.

60. "Trusted third party" means (a) an authority or its agent, trusted by other actors with respect to other activities (e.g., security related activities). Source: Rec. ITU-T X.1254; (b) an entity accepted by all parties to a transaction as an impartial and trustworthy intermediary to facilitate interactions between and among the parties.

61. "User" means (a) a subject of a credential; a consumer of the services offered by a relying party; (b) any entity that makes use of a resource, e.g., system, equipment, terminal, process, application, or corporate network. Source: Rec. ITU-T X.1252.

62. "Validation" means the process of verifying and confirming that an identity credential is valid (e.g., that it has not expired or been revoked).

63. "Verification" means (a) the process of checking information by comparing the provided information with previously corroborated information. Source: Rec. ITU-T X.1254; (b) the process or instance of establishing the authenticity of something. Note: verification of (identity) information may encompass examination with respect to validity, correct source, original, (unaltered), correctness, binding to the entity, etc. Source: Rec. ITU-T X.1252.

B. Definitions relevant to trust services

64. The following definitions may be particularly relevant in discussions on the legal aspects of trust services. However, a number of the definitions listed as relevant to the discussions on legal aspects of identity management may also be relevant for the discussions on the legal aspects of trust services (see above, para. 8).

65. "Certificate for website authentication" means an attestation that makes it possible to authenticate a website and links the website to the natural or legal person to whom the certificate is issued. Source: eIDAS, article 3(38). (See also A/CN.9/WG.IV/WP.144, para. 20.)

66. "Certification service provider" means a person that issues certificates and may provide other services related to electronic signatures. Source: UNCITRAL Model Law on Electronic Signatures, article 2(e).[5]

67. "Electronic document" means any content stored in electronic form, in particular text or sound, visual or audiovisual recording. Source: eIDAS, article 3(35). (See also A/CN.9/WG.IV/WP.144, para. 20.)

68. "Electronic registered delivery service" means a service that makes it possible to transmit data between third parties by electronic means and provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data, and that protects transmitted data against the risk of loss, theft, damage or any unauthorized alterations. Source: eIDAS, article 3(36). (See also A/CN.9/WG.IV/WP.144, para. 20.)

69. "Electronic seal" means data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity. Source: eIDAS, article 3(25). (See also A/CN.9/WG.IV/WP.144, para. 20.)

70. "Electronic signature" means (a) data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign. Source: eIDAS, article 3(10) (see also A/CN.9/WG.IV/WP.144, para. 20); (b) data in electronic form in, affixed to or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory's approval of the information contained in the data message. Source: UNCITRAL Model Law on Electronic Signatures, article 2(a). Note: article 9(3)(a) of the United Nations Convention on the Use of Electronic Communications in International Contracts (New York, 2005)[6] refers to indication of the signatory's intention in respect of the information contained in the electronic communication.

71. "Electronic time stamp" means data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time. Source: eIDAS, article 3(33). (See also A/CN.9/WG.IV/WP.144, para. 20.)

72. "Qualified trust service" means a trust service that meets the applicable requirements laid down in this [Convention] [Model Law]. Source: A/CN.9/WG.IV/WP.144, para. 20.

73. "Relying party" means (a) a person that may act on the basis of a certificate or an electronic signature. Source: UNCITRAL Model Law on Electronic Signatures, article 2(f); (b) a natural or legal person that relies upon an electronic identification or a trust service. Source: A/CN.9/WG.IV/WP.144, para. 20.

74. "Signatory" means (a) a natural person who creates an electronic signature. Source: eIDAS, article 3(9). (See also A/CN.9/WG.IV/WP.144, para. 20); (b) a person that holds signature creation data and acts either on its own behalf or on behalf of the

[5] United Nations publication, Sales No. E.02.V.8.

[6] General Assembly resolution 60/21, annex.

person it represents. Source: UNCITRAL Model Law on Electronic Signatures, article 2(d).

75. "Trust service" means an electronic service normally provided for remuneration which consists of: (a) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or (b) the creation, verification and validation of certificates for website authentication; or (c) the preservation of electronic signatures, seals or certificates related to those services. Source: eIDAS, article 3(16).

76. "Trust service provider" means a natural or a legal person who provides one or more trust services [either as a qualified or as a non-qualified trust service provider]. Source: eIDAS, article 3(19). (See also A/CN.9/WG.IV/WP.144, para. 20.)

77. "Time stamp" means a reliable time variant parameter which denotes a point in time with respect to a common reference. Source: Rec. ITU-T X.1254.

78. "Validation" means the process of verifying and confirming that an electronic signature or a seal is valid. Source: eIDAS, article 3(41). (See also A/CN.9/WG.IV/WP.144, para. 20.)